What is claimed is:

1. A computerized system for storing and publishing encryption keys for an electronic encryption system that sends encrypted transmissions between a sender and a recipient comprising:

a first computer readable medium having a first communications connection for electronic communications over a network;

a first storage area embodied within said first computer readable medium;

a second computer readable medium having a second communications connection for electronic communications over a network for providing electronic communications with said first computer readable medium;

a second database having a second set of public keys embodied in said second computer readable medium;

a first set of computer readable instructions embodied within said first computer readable medium for:

receiving a request for a recipient's public key from the sender through said first communications connection,

querying said first storage area for the requested recipient's public key;

transmitting the recipient's public key to the sender if the recipient's public key is found within said first storage area, and,

transmitting a second request for the recipient's public key to said second computer readable medium if the recipient's public key is not found in said first storage area so that the sender is either provided with the recipient's public key

or said second request is sent to said second computer readable medium requesting the recipient's public key.

2. The system of claim 1 wherein:

said second communications connection allows for electronic communications with a root server; and,

a second set of computer readable instructions embodied within said second computer readable medium for:

receiving a said second request for the recipient's public key from said first set of computer readable instructions,

querying said second database for the recipient's public key,

transmitting the recipient's public key to said first computer readable medium if the recipient's public key is found in said second database,

transmitting an upstream request to said root server for the recipient's public key is not found in said second database;

receiving the recipient's public key if the recipients' public key is provided by said root server;

receiving a pointer to the recipient's public key if the pointer to the public key is provided by said root server; and,

retrieving the recipient's public key from a location provided by the root pointer to the recipient's public key if the pointer to the recipient's public key is provided to said first computer readable medium.

3. The system of claim 2 including:

a root computer readable medium having a root communications

connection for communicating with the network and said second computer readable medium;

a root database embodied in said root computer readable medium containing pointers to all public keys of the encryption system;

a set of computer readable root instructions embodied in said root computer readable medium for:

receiving said upstream request from said second set of computer readable instructions,

querying said root database for the pointer to the recipient's public key,

transmitting the pointer of the recipient's public key to said second computer readable medium if the pointer to the recipient's public key is found within said root database, and,

transmitting a not found statement to said second computer readable medium if the pointer to the recipient's public key is not found in said root database so that the sender can be provided with the recipient's public key or the sender can be informed that the recipient's public key can not be found.

4. The system of claim 3 including:

said set of computer readable root instructions includes instruction for transmitting said key server address of the next key computer readable medium down the hierarchy having a pointer to the recipient's public key.

5. The system of claim 3 including:

a plurality of key computer readable mediums arranged in a hierarchy having public keys stored within said computer readable mediums;

a plurality of key server address associated with each of said key computer readable mediums representing the location of said key computer readable mediums within said hierarchy; and,

said set of computer readable root instructions includes instruction for transmitting said key server address of the next key computer readable medium down the hierarchy having the recipient's public key.

6. The system of claim 2 including:

a root server cluster having a root computer readable medium and a root communications connection for communicating with the network and said second computer readable medium;

a root database embodied within said root server cluster containing pointers to all of the public keys of the encryption system;

a set of computer readable medium root instructions embodied in said root server cluster for:

receiving said upstream request from said second set of computer readable instructions,

querying said root database for the requested recipient's public key,

transmitting the recipient's public key to said second computer readable medium if the recipient's public key is found within said root database, and,

transmitting a not found statement to said second computer readable medium if the recipient's public key is not found in said root database so that the sender can be provided with the recipient's public key or the sender can be informed that the recipient's public key can not be found.

7. The system of claim 1 wherein said first set of computer readable instructions includes instruction for:

receiving the recipient's public key from said second computer readable medium if the recipient's public key is found within said second database; and,

transmitting the recipient's public key to the sender if the recipient's public key is received from said second computer readable medium so that the sender may encrypt a transmission with the recipient's public key.

8. The system of claim 7 wherein said first set of computer readable instructions includes instruction for storing the recipient's public key within said first computer readable medium upon receipt of the recipient's public key so that the recipient's public key is available upon subsequent requests received for the recipient's public key.

9. The system of claim 1 including:

a temporary storage section contained within said first computer readable medium;, and,

said first set of computer readable instructions include instruction for:

receiving the recipient's public key from said second computer readable medium if said second computer readable medium provides the recipient public key; and,

storing the recipient's public key within said temporary storage section upon receipt of the recipient's public key from said second computer readable medium so that the recipient's public key is available from said temporary storage section according to the subsequent request for the recipient's public key.

10. The system of claim 9 wherein said first set of computer readable instructions include instruction for deleting the received recipient's public key from said temporary storage section upon the expiration of a predetermined period of time.

11. The system of claim 9 wherein said first set of computer readable instructions include instruction for deleting the received recipient's public key from said temporary storage section according to a set of predetermined criteria.

12. A computerized system for storing and publishing encryption keys for an electronic encryption system for sending encrypted transmissions between a sender and a recipient comprising:

a first computer readable medium;

a communications connection in communication with said first computer readable medium for transmitting and receiving electronic information on a network;

a database embodied in said first computer readable medium having public keys;

a set of computer readable instructions embodied in said first computer readable medium for:

receiving a request from a requester for the recipient's public key,

querying said database for said recipient's public key,

transmitting said public key to the requester if the recipient's public key is found in said database, and,

transmitting an upstream request to an upstream server for the recipient's public key if said public key is not found in said database so that said

sender is either provided with the recipient's public key or the upstream request for the recipient's public key is sent upstream.

13. The system of claim 12 including:

a root computer readable medium having a root communications connection for communicating with the network and said first computer readable medium;

a root database containing pointers to all public keys of the encryption system;

a set of computer readable root instructions embodied in said root computer readable medium for:

receiving an upstream request for the recipient's public key to said computer readable medium,

transmitting the pointer to the recipient's public key from said first computer readable medium if the pointer to the recipient's public key is found within said root database, and,

transmitting a not found statement to said computer readable medium if the pointer to the recipient's public key is not found in said root database.

14. The system of claim 12 including:

a root computer readable medium having a root communications connection for communicating with the network and said first computer readable medium;

a plurality of key computer readable mediums arranged in a hierarchy having public keys stored within said key computer readable mediums in

communication with said root computer readable medium and said first computer readable mediums;

a plurality of key server addresses associated with each of said computer readable mediums representing the location of said key computer readable mediums within said hierarchy; and,

a set of computer readable root instructions embodied in said root computer readable medium for:

receiving an upstream request for the recipient's public key,

querying said root computer readable for the recipient's public key; ;and,

transmitting the key server address of the next key computer readable medium down the hierarchy if the recipient's public key was not found within said root computer readable medium.

15. The system of claim 14 wherein said computer readable instructions include instruction for transmitting a final request to a location according to receiving the pointer of the recipient's public key so that said computer readable instructions can discover the recipient's public key at the pointer location.

16. The system of claim 15 having a root server cluster embodying said root computer readable medium.

17. The system of claim 12 including:

a temporary storage section contained with said computer readable medium; and,

said set of computer readable instructions include instruction for:

receiving the recipient's public key from said upstream server, and,

storing the recipient's public key within said temporary storage section upon receipt of the recipient's public key from said upstream server so that the recipient's public key is available to said computer readable medium.

18. A computerized system for storing and publishing encryption keys for an electronic encryption system that sends encrypted transmissions between a sender and a recipient comprising:

a first computer readable medium having a first communications connection for electronic communications over a network;

a second computer readable medium having a second communications connection for electronic communications over a network for providing electronic communications with said first computer readable medium;

a database having a set of public keys and public key address pointers embodied in said second computer readable medium;

a first set of computer readable instructions embodied within said first computer readable medium for:

receiving a request for a recipient's public key from a requester through said first communications connection,

querying said first computer readable medium for the requested recipient's public key;

querying said first computer readable medium for the address pointer if the recipient's public key if the recipient's public key was not found,

transmitting a second request to said second database for the requested recipient's public key if said address pointer of the recipient's public key or the recipient's public key was not found,

receiving the recipient's public key if the recipient's public key is found on said database,

receiving the pointer to the recipient's public key if the pointer of the recipient's public key is found on said database,

receiving the recipient's public key according to the address pointer if the recipient's public key is received, and,

transmitting the recipient's public key to the sender if the recipient's public key is received.

19. The system of claim 14 including:

a root computer readable medium having a root communications connection with said network, first computer readable medium and second computer readable medium;

a root database containing address pointers to all public keys of the encryption system;

a set of computer readable root instructions embodied in said root computer readable medium for:

receiving the request for the address pointer of the recipient's public key from said first set of computer readable instructions,

querying said root database for the pointer to the recipient's public key,

transmitting the pointer to the recipient's public key to said first computer readable medium if the address pointer to the recipient's public key is found within said root database so that the sender can be provided the public key of the recipient to send an encrypted message, and,

transmitting a not found statement to said first set of computer readable instructions so that the sender can be informed that the recipient's public key can not be found.

20. The system of claim 18 where said first set of computer readable instructions include instruction for storing the address pointer of the recipient's public key within said first computer readable medium so that said first set of computer readable instructions can retrieve the recipient's public key according to subsequent requests for the recipient's public key.

21. The system of claim 19 wherein said received address pointer of the recipient's public key is removed from said first computer readable medium according to predetermined criteria.